## REMARKS

Claims 23-60 stand rejected. Claims 23 and 38 have been amended. New claims 61-62 have been added. No new matter has been added. The amendment and the new claims are supported by the specification. Claims 23-62 are presently pending. In view of the foregoing amendments and the following remarks, Applicant respectfully submits that all of the presently pending claims are allowable. Reconsideration of the Application is respectfully requested.

### 1. Rejection of claims 23-60 (35 U.S.C. § 102(e))

Claims 23 and 38 were amended to improve clarity. The amendment was not intended to change the scope of the claims. Claims 23-60 were rejected under 35 U.S.C. § 102(e), the Examiner alleging that these claims are unpatentable over U.S. Patent No. 6,149,522 to Alcorn et al. ("Alcorn"). The Applicant respectfully traverses this assertion and submits that the rejections should be withdrawn for at least the following reasons.

To anticipate a claim, the reference must teach every element of the claim. *See* MPEP 2131. The identical invention must be shown in as complete detail as is contained in the claim. *See id.* (citing *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236 (Fed. Cir. 1989)). Because Alcorn does not teach all the elements of the claims, withdrawal of the 35 U.S.C. § 102(e) rejection is respectfully requested.

Claim 43 recites, in relevant part, "decrypting the second encrypted electronic information into a second decrypted electronic information at the gaming terminal with at least the first resident security key and the second non-resident security key." Applicant respectfully submits that this claim element is neither taught nor suggested by Alcorn.

Alcorn severally describes decrypting a first signature with a first decryption key and then decrypting a second signature with a second decryption key. Thus, Alcorn fails to

describe decrypting a second encrypted electronic information with at least a first resident security key ***and*** a second non-resident security key. Alcorn describes two authentication programs. The first authentication program validates an anchor application. (Col. 12, lines 33-35). If the anchor application is valid, the anchor application is loaded into main memory. The second authentication program of the anchor application is used to authenticate any further applications accessed or received, for example, the game data set or game modifying data set. (Col. 12, lines 37-53).

The authentication program is described in Fig. 5 of Alcorn. (Col. 8, lines 59-60). The authentication procedure described in Fig. 5 is implemented in the first secure loader and the second secure loader depicted in Fig. 6. (Col. 10, lines 14-16 and lines 39-41). The authentication procedure of Fig. 5 decrypts an encrypted data set signature 37 with a public decryption key 34. The decrypted message digest 47 is compared with a computed message digest 46. If the two message digests match, the game data set is considered authentic. (Col. 9, lines 3-10).

Thus, Alcorn's two signatures are separately decrypted by using two separate keys. Alcorn does not describe decrypting an encrypted electronic information with at least the first resident security key and the second non-resident security key.

In addition, claim 43 recites, in relevant part, "replacing a first resident electronic information at the gaming terminal with the second decrypted electronic information." In contrast, Alcorn's decrypted first and second signatures are compared with the first and second computed message digest, respectively. Alcorn fails to describe replacing "a first resident electronic information" with decrypted information. Thus, Alcorn fails to anticipate claim 43 and the rejection should be withdrawn.

Claims 44-60 depend from claim 43 and thus allowable over Alcorn for at least the same reasons as claim 43.

In addition, claim 48 recites, in relevant part, "wherein the transmitting is

accomplished with a physical electronic key removably attached to the gaming terminal." Col. 10, lines 28-33 of Alcorn generally describes a ROM 54 kept on file in a secure location to be compared against a ROM removed from a gaming machine. Thus, the ROM 54 does not transmit the second encrypted electronic information, but is used for storage purposes. Nor is the ROM 54 a physical electronic key removably attached to the gaming terminal because it is stored in a secure location and not at the gaming terminal. Thus, Alcorn fails to anticipate claim 48 and the rejection should be withdrawn.

In addition, claim 49 recites, in relevant part, "decrypting an encrypted master reset component in the gaming terminal with the second non-resident security key." Col. 12, lines 52-62 of Alcorn generally describes determining whether a game data set or game-modifying data set is valid, and if so, loading the new game data set or game modifying data set. A signature is decrypted as part of the validation process. Alcorn fails to describe or suggest an encrypted master reset component or decrypting the encrypted master reset component. Thus, Alcorn fails to anticipate claim 49 and the rejection should be withdrawn.

In addition, claim 50 recites, in relevant part, "determining a version information of the second encrypted electronic information with an information in the second non-resident security key." Col. 12, lines 52-62 and col. 9, lines 17-40 of Alcorn generally describes decrypting two signatures and validating data with the decrypted signatures. Neither of the two signatures, which are decrypted by the game terminal, comprises version information. Thus, Alcorn fails to anticipate claim 50 and the rejection should be withdrawn.

In addition, claim 52 recites, in relevant part, "the second decrypted information comprises game application code." Col. 12, lines 52-62 of Alcorn generally describes determining whether a game data set or game-modifying data set is valid, and if so, loading the new game data set or game modifying data set. A signature is decrypted as part of the validation process. Alcorn does not suggest that either of the two signatures, which are decrypted, comprises game application code. Thus, Alcorn fails to anticipate claim 52 and the rejection should be withdrawn.

In addition, claim 53 recites, in relevant part, "the second decrypted information comprises game system modules." Col. 12, lines 52-62 of Alcorn generally describes determining whether a game data set or game-modifying data set is valid, and if so, loading the new game data set or game modifying data set. A signature is decrypted as part of the validation process. Alcorn does not describe that either of the two signatures, which are decrypted, comprises game system modules. Thus, Alcorn fails to anticipate claim 53 and the rejection should be withdrawn.

In addition, claim 54 recites, in relevant part, "the second decrypted information comprises game graphics and audio files." Col. 7, line 65 through col. 8, line 14 of Alcorn generally describes ROMs 29 and 30. The ROMs contain a system initialization code, an authentication program, an initial portion of the loader programs, game image and sound data, rules of game play and the like, and the signature associated with each particular casino game. Alcorn does not describe that the signature, which is encrypted, comprises game graphics and audio files. The game image and sound data described by Alcorn is not what Alcorn indicates is to be decrypted, they cannot be the claimed second decrypted information. Thus, Alcorn fails to anticipate claim 54 and the rejection should be withdrawn.

In addition, claim 55 recites, in relevant part, "the second decrypted information comprises new release game software files." Col. 12, lines 52-62 of Alcorn generally describes determining whether a game data set or game-modifying data set is valid, and if so, loading the new game data set or game modifying data set. A signature is decrypted as part of the validation process. Alcorn does not describe that either of the two signatures, which are decrypted, comprises new release game software files. Thus, Alcorn fails to anticipate claim 55 and the rejection should be withdrawn.

In addition, claim 56 recites, in relevant part, "transmitting a third encrypted electronic information from the host device" and "receiving a third non-resident security key with the second encrypted electronic information at the gaming terminal." Col. 11, lines 3-29 of Alcorn generally describe a second authentication program of an anchor application

decrypting and using a second signature. Even assuming, for the sake of argument, that the third encrypted electronic information may have "essentially the same meaning" as the second encrypted electronic information as asserted by the Office Action, an anticipation rejection requires each and every element of the claim be disclosed in the reference. Alcorn fails to describe a third encrypted electronic information. Thus, Alcorn fails to anticipate claim 56 and the rejection should be withdrawn.

In addition, claim 57 recites, in relevant part, "packaging the third non-resident security key and the second encrypted electronic information into one file." Col. 4, lines 43-67 of Alcorn generally describe a program or fixed data set preparation phase, wherein a first abbreviated bit string is computed and encrypted to provide an encrypted signature of the program. Alcorn fails to describe, nor even suggest, packaging a security key together with an encrypted information into one file. Thus, Alcorn fails to anticipate claim 57 and the rejection should be withdrawn.

Similar to claim 43, claim 23 recites, in relevant part, "the second decrypted electronic information decrypted from the second encrypted electronic information by the decrypting component with at least the first resident security key and the second non-resident security key." Because Alcorn fails to describe decrypting a second encrypted electronic information with at least a first resident security key and a second non-resident security key, Alcorn cannot anticipate claim 23.

In addition, claim 23 also recites, in relevant part, "a second decrypted electronic information to replace the first resident electronic information." Because Alcorn fails to describe replacing "a first resident electronic information" with decrypted information, Alcorn cannot anticipate claim 23.

Thus, Applicant respectfully submits the anticipation rejection of claim 23 should be withdrawn for at least similar reasons to claim 43.

Claims 24-42 depend from claim 23 and thus should be patentable over Alcorn for at

least the same reasons as claim 23.

In addition, claim 29 recites, in relevant part, "a removable storage media removably attached to the gaming terminal, the removable storage media configured to receive and to transmit electronic information." Similar to the discussion of claim 48, Alcorn fails to describe this limitation.

In addition, claim 30 recites, in relevant part, "a removable storage media removably attached to the gaming terminal, the removable storage media configured as a non-network connection." Similar to the discussion of claim 48, Alcorn fails to describe this limitation.

In addition, claim 31 recites, in relevant part, "an encrypted master reset component, the decrypting component configured to decrypt the encrypted master reset component with the second non-resident security key." Similar to the discussion of claim 49, Alcorn fails to describe this limitation.

In addition, claim 32 recites, in relevant part, "the second non-resident security key comprises information to determine a version information of the second encrypted electronic information." Similar to the discussion of claim 50, Alcorn fails to describe this limitation.

In addition, claim 34 recites, in relevant part, "the second decrypted information comprises game application code." Similar to the discussion of claim 52, Alcorn fails to describe this limitation.

In addition, claim 35 recites, in relevant part, "the second decrypted information comprises game system modules." Similar to the discussion of claim 53, Alcorn fails to describe this limitation.

In addition, claim 36 recites, in relevant part, "the second decrypted information comprises game graphics and audio files." Similar to the discussion of claim 54, Alcorn fails to describe this limitation.

In addition, claim 37 recites, in relevant part, "the second decrypted information

comprises new release game software files." Similar to the discussion of claim 55, Alcorn fails to describe this limitation.

In addition, claim 38 recites, in relevant part, "a third encrypted electronic information" and "a third non-resident security key." Similar to the discussion of claim 56, Alcorn fails to describe this limitation.

In addition, claim 39 recites, in relevant part, "wherein the third non-resident security key is packaged with the second encrypted electronic information into one file for transmission to the gaming terminal." Similar to the discussion of claim 57, Alcorn fails to describe this limitation.

For at least the foregoing reasons, Applicant submits that Claims 23-60 are allowable and respectfully request withdrawal the 35 U.S.C. § 102(e) rejection.

**2. New Claims 61 and 62**

New claim 61 depends from claim 23, and is therefore allowable for at least similar reasons as claim 23. In addition, new claim 61 recites, in relevant part, "decrypt the second encrypted information into an interim result with the first resident security key" and "decrypt the interim result into the second decrypted information with the second non-resident security key." Alcorn fails to describe an interim result which is then decrypted.

The result of Alcorn's first authentication program is a decrypted message digest compared with a computed message digest to determine whether the anchor application is valid. The decrypted message digest is not further decrypted.

Similarly, claim 62 depends from claim 43, and is therefore allowable for at least similar reasons as claim 43. In addition, new claim 62 recites, in relevant part, "decrypting the second encrypted electronic information into an interim result with the first resident security key at the gaming terminal" and "decrypting the interim result into the second decrypted electronic information with the second non-resident security key at the gaming

terminal." Thus, claim 62 should be allowable for at least similar reasons as claim 61.

## CONCLUSION

In view of the above amendments and remarks, it is respectfully submitted that all of the presently pending claims are allowable. All issues raised by the Examiner having been addressed, an early and favorable action on the merits is earnestly solicited.

The Office is authorized to charge any fees associated with this Amendment to Kenyon & Kenyon Deposit Account No. 11-0600.

Respectfully Submitted,

KENYON & KENYON

Dated: Dec. 21, 2005

By: _____

Andrew L. Reibman
(Reg. No. 47,893)

One Broadway
New York, NY 10004
(212) 425-7200

**CUSTOMER NO. 26646**